REMARKS

The present application was filed on January 23, 2004 with claims 1 through 16. Claims 1 through 16 are presently pending in the above-identified patent application. Claims 1 and 13 are proposed to be amended and claims 2 and 14 are proposed to be cancelled, without prejudice, herein.

In the Office Action, the Examiner rejected claims 1-16 under 35 U.S.C. §102(b) as being anticipated by Takaragi et al. (United States Patent Number 6,141,421).

Independent Claims 1, 8, 10, 11, 13 and 15

Independent claims 1, 8, 10, 11, 13 and 15 were rejected under 35 U.S.C. §102(b) as being anticipated by Takaragi et al. Regarding claims 1 and 13, the Examiner asserts that Takaragi discloses generating a compressed Rabin signature based on a continued fraction expansion of s/n (col. 14, lines 21-32, and col. 15, lines 9-15). Regarding claims 8 and 15, the Examiner asserts that Takaragi discloses applying a message formatting function, h, to the message, m, to computing h(m) (col. 10, lines 27-50); computing a value, t, as $h(m)v^2$ mod n (col. 10, lines 50-65; and col. 14, lines 32-57); obtaining a value, w, as a square root of the value, t (col. 11, lines 1-24); and computing a signature value, s, as w/v mod n (col. 11, lines 1-24).

Applicant notes that independent claims 1 and 13 have been amended to incorporate the limitations of claim 2. In rejecting claim 2, the Examiner asserted that Takaragi discloses computing principal convergents, u_i/v_i, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined (FIGS. 3-4; col. 8, lines 3-5); establishing an index *l*, such that $v_l < \sqrt{n} < v_{l+1}$ (FIG. 3; col. 8, lines 6-20); and generating a compressed Rabin signature (v_l, m) for a message, m (FIG. 3; col. 8, lines 21-28). Applicants note, however, that FIGS. 3-12 and columns 8-11 of Takaragi are directed to *processing the original message*; FIGS. 3-12 and columns 8-11 are *not* directed to *compressing or decompressing a Rabin signature*.

Thus, Takaragi does not disclose or suggest generating a compressed Rabin signature based on a continued fraction expansion of s/n, wherein said continued fraction expansion of s/n further comprises the steps of computing principal convergents, u_i/v_i, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined; establishing an index *l*, such that $v_l < \sqrt{n} < v_{l+1}$; and generating a compressed Rabin signature (v_l, m) for a message, m, as required by independent claims 1 and

13, as amended, does not disclose or suggest applying a message formatting function, h, to the message, m, to computing h(m); computing a value, t, as $h(m)v^2$ mod n; obtaining a value, w, as a square root of the value, t; computing a signature value, s, as w/v mod n; and providing a decompressed signature (s,m), as required by independent claims 8 and 15, does not disclose or suggest computing principal convergents, u_i/v_i, of the continued fraction expansion of s/n; establishing an index l, such that $v_l < n^{(1-1/e)} \leq v_{l+1}$; and generating a compressed signature (v_l, m), as required by independent claim 10, and does not disclose or suggest applying a message formatting function, h, to the message, m, to computing h(m); computing a value, t, as $h(m)v^e$ mod n; determining whether the values t or t-n have an e^{th} root over integer values; computing a value, w, as the e^{th} root; and computing the decompressed signature (w/v mod n, m), as required by independent claim 11.

Dependent Claims 2-7, 12, 14 and 16

Claims 2-7, 12, 14, and 16 are dependent on independent claims 1, 8, 11, 13, and 15, and are therefore patentably distinguished over Takaragi et al. because of their dependency from amended independent claims 1, 8, 11, 13 and 15 for the reasons set forth above, as well as other elements these claims add in combination to their base claim.

Conclusion

All of the pending claims following entry of the amendments, i.e., claims 1-16, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Respectfully submitted,

Date: December 23, 2008

Kevin M. Mason
Attorney for Applicants
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06824
(203) 255-6560